Docket No.: 0081004.00167US2
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Ari JUELS	Confirmation No.:	6866
Application No.:	09/802,278	Art Unit:	3621
Filed:	March 8, 2001	Examiner:	P. E. Elisca
Title:	TARGETED DELIVERY OF INFORMATIONAL CONTENT WITH PRIVACY PROTECTION		

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

This brief is filed within one month of the mailing date of the Notice of Panel Decision from Pre-Appeal Brief Review (with a proper extension of time under 37 CFR §1.136(a)), and is in furtherance of said Notice of Appeal.

The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

I.   REAL PARTY IN INTEREST

The real party in interest for this appeal is RSA Security Inc, the assignee of the present application. The assignment from inventor Ari Juels to RSA Security Inc., was recorded on June 20, 2001, at Reel 011920, Frame 0207.

II.   RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings, which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III.   STATUS OF CLAIMS

Claims 1 through 23 are pending in the application. None of the pending claims have been canceled, and none of the pending claims have been withdrawn from consideration. Claims 18-23 have been allowed. Claims 1-17 have been rejected. Claims 1-17 are on appeal.

IV.   STATUS OF AMENDMENTS

None of the pending claims have been amended.

The first Office Action (non-final) of June 12, 2003 rejected claims 1-17 under 35 U.S.C. 102(e) as anticipated by U.S. Patent No. 6,460,036 (Herz) and allowed claims 18-23. A

Response filed December 12, 2003 presented arguments against the rejections, without amending the claims.

The second Office Action (Final) of March 12, 2004 maintained the rejections from the first Office Action. A Response filed on September 13, 2004, along with a Request for Continued Examination (RCE), presented arguments against the rejections, without amending the claims.

The third Office Action (non-final) of October 12, 2004 maintained the rejections from the first Office Action. Following a telephonic Examiners Interview conducted on December 2, 2004, a Response to the third Office Action was filed on February 14, 2005 that summarized the arguments presented in the Interview, without amending the claims.

The fourth Office Action (non-final) of May 11, 2005 withdrew the rejections of claims 1-17 under 35 U.S.C. 102(e) as anticipated by U.S. Patent No. 6,460,036 to Herz (Herz), and rejected claims 1-17 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,460,036 (Herz) in view of U.S. Patent No. 6,249,772 to Walker et al. (Walker). A Response filed on October 7, 2005 presented arguments against the rejections, without amending the claims.

The fifth Office Action (Final) of December 9, 2005 maintained the rejections presented in the fourth Office Action. Following a telephonic Examiners Interview conducted on February 15, 2006, a Response to the second Office Action was filed on March 8, 2006 that summarized the arguments presented in the Interview, without amending the claims.

An Advisory Action was mailed on March 24, 2006. A Pre-Appeal Brief Request for Review was filed on June 9, 2006. A Notice of Panel Decision from Pre-Appeal Brief Review was mailed on August 11, 2006, with instructions to proceed to Board of Patent Appeals and Interferences.

A copy of the pending claims is attached as Appendix A.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

Advertising over a network is well known and has been in practice for some time. For example, marketers of products and services have advertised to consumers via broadcast television networks for years. Such advertising, however, cannot be directed to a particular

consumer or category of consumers due to the nature of the broadcast network. The broadcast advertising consequently reaches consumers who have no interest in the advertised product or service, and the advertiser must bear the cost of advertising to an unnecessarily large audience.

The interactive nature of more recent networks, such as the Internet, provides an opportunity for targeted advertising. Advertisers can collect information about the consumer, such as which Internet sites the consumer visits, consumption patterns and demographic data, and use the information to craft specific advertisements to be targeted to particular consumers.

With targeted advertising, consumers are less likely to receive unwanted or irrelevant advertisements. Further, a consumer does not need to filter large amounts of advertising to find the advertisements in which he or she is interested. And advertisers can concentrate their resources only on advertising to which the consumer is likely to pay attention.

Although targeted advertising clearly has social and economic benefits, it also comes with potential privacy issues. Since the advertiser needs to collect information concerning the consumer in order to tailor the advertising, the potential exists for misuse of that information.

In general, the independent claims 1, 3 and 7 each recite a method for enabling use of detailed consumer profiles for delivering targeted information, while protecting these profiles from disclosure to information providers or hostile third parties. Rather than gathering data about a consumer in order to decide which information to send him or her, an information provider makes use of a client side executable software module called a "negotiant function." U.S. Patent Application Publication US 2002/0026345, paragraph [0010].

The negotiant function is an element of each of the independent claims 1, 3 and 7. The negotiant function requests elements of information from the information provider. These elements of information are tailored to the characteristics of the consumer. *Id*. at paragraph [0011].

Claim 1 recites a method of retrieving "targeted information" while protecting consumer privacy. In general, the method recites the steps of (i) providing "elements of information," (ii) specifying a negotiant function, and (iii) "distributing" the negotiant function to a consumer for "execution by the consumer." The input to the negotiant function is elements of data associated with a consumer. The output of the negotiant function is an information request that designates,

4

based on the input, at least one of the elements of information referred to in step (i) to present to the consumer. App. A, at p.1.

Claim 3 recites a method of retrieving "targeted information" while protecting consumer privacy. In general, the method recites the steps of (i) receiving a negotiant function and (ii) executing the negotiant function. Upon execution, the negotiant function generates an information request. The information request designates at least one element of information from among a plurality of elements of information.

Claim 7 recites a method of retrieving "targeted information" while protecting consumer privacy. In general, the method recites the steps of (i) distributing a negotiant function to consumers and (ii) receiving information requests associated with the consumers. As described above for claim 1, inputs to the negotiant function are elements of data associated with a consumer, and outputs of the negotiant function are information requests. Claim 7 recites generating each information request associated with a consumer by applying the negotiant function to data associated with the consumer.

VI.   GROUNDS OF OBJECTION TO BE REVIEWED ON APPEAL

A.   Rejection of claims 1-17 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,460,036 issued to Herz (Herz) in view of U.S. Patent No. 6,249,772 issued to Walker et al. (Walker).

VII.   ARGUMENT

Claims 1-17 are patentable over Herz in view of Walker, because the combination of Herz and Walker fails to teach distributing (or receiving) a negotiant function to a consumer for execution by the consumer. Herz describes an exchange that takes place between two servers, which does not involve or require any <u>execution</u> on the part of a consumer or client. Further, Herz does not teach or suggest <u>distributing</u> a negotiant function to a consumer.

Walker does not supply that which is missing from Herz. Walker describes a system that allows a user to identify and select, through a computer-based web browser, a product at a local retailer. The Walker system allows a user to negotiate a price for the product through the

browser, but does not teach or suggest distributing a negotiant function to a consumer, or execution of the negotiant function.

Claims 1-17 recite a "negotiant" function, and not a "negotiation" function. The specification describes a "negotiant" function for one embodiment as a function that takes information related to a consumer as input, and produces an output related to an advertisement selection. The output can be an actual advertisement selection, or information that can be used to derive an advertisement selection. The negotiant function therefore acts as a client-side proxy to protect consumer data, and also directs the targeting of information. U.S. Patent Application Publication US 2002/0026345, paragraph [0039]. The negotiant function as recited in the rejected claims does not provide a "negotiation," as that term is used in the cited art of Herz and Walker.

A.   **Rejection of claims 1-17 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,460,036 issued to Herz (Herz) in view of U.S. Patent No. 6,249,772 issued to Walker et al. (Walker).**

1. <u>Claim 1</u>

The Examiner rejects claims 1-17 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,460,036 issued to Herz in view of U.S. Patent No. 6,249,772 issued to Walker. Claim 1 is patentable over the combination of Herz and Walker because the combination of Herz and Walker fails to teach distributing a negotiant function to a consumer for execution by the consumer.

Claim 1 describes a negotiant function as a function that accepts elements of data associated with a consumer as input, and produces an information request as output. The specification supports this description of a negotiant function (see for example paragraphs [0038]-[0040] of U.S. Patent Application Publication US 2002/0026345 A1).

Neither Herz nor Walker, alone or in combination, teaches a negotiant function. The Examiner cites Herz as teaching "distributing the negotiant function":

> When necessary in order to act on embedded message M1, server <u>S4 may exchange or be caused to exchange</u> further signed and optionally encrypted messages <u>with proxy server S2</u>, still over normal point to point connections, <u>in order to negotiate the</u>

> release of user-specific information and credentials from proxy server S2. (Herz, col. 39, lines 47-53, emphasis added)

This "negotiation" is not a negotiant function as set forth in claim 1, and does not involve the user (*i.e.,* the ultimate consumer in Herz) at all. The "negotiation" is simply an exchange that takes place between server S2 and server S4, neither of which is the consumer. Herz further teaches that after the negotiation between servers S2 and S4, the server S4 may send a response M2 to the user, via server S2, *i.e.,*

> If proxy server S2 has sent a message to a server S4 and S4 has created a response M2 to message M1 to be sent to the user, then server S4 transmits the response M2 to the proxy server S2 using normal point-to-point connections. (Herz, col. 39, lines 61-65).

But sending the response M2 occurs after and as a result of the negotiation between servers S2 and S4. Thus the negotiation taught by Herz is not a negotiant function, nor is it "for execution by the user," as is required by claim 1.

To address this deficiency of Herz, the Examiner relies on the Walker patent:

> Based on the interview conducted on 12/02/2004, Applicant's representative argued that the prior art of record (Herz 036") fails to disclose distributing the negotiation function to a consumer for execution by said consumer. Whereas in Herz the negotiation has been done by two servers S2 and S4 but not by the consumer. However, the Examiner has made an updated search and found new prior art (Walker et al 772"). (Office Action mailed December 9, 2005; page 3).

The Examiner characterizes Walker as teaching "a system/method wherein a consumer negotiates a price for a selected product, [so that] the consumer is assured that he will actually receive the product. (see., abstract, col 10, lines 35-45)." This teaching from Walker does not supply that which is missing from Herz. It does not teach the "distributing the negotiant function to a consumer for execution by the consumer" limitation of claim 1.

Walker's system allows a user to identify and select, through a computer-based web browser, a product at a local retailer:

> In system 100, when user computer 102 identifies a product online via an interactive web-browser, user computer 102 is then provided a price established by a manufacturer and transmitted from central controller 110. Thereafter, a user/customer can purchase and pick up the selected product from a retailer, selected from the list of retailers who have agreed to honor the price set by the manufacturer and transmitted to user computer 102, regardless of the retailer's normal price for such product. Accordingly, system 100 allows user computer 102 to log onto a central controller via network 106 and "lock-in" a price for an item which may be

7

different from the shelf price posted at the local store from which the customer chooses to subsequently purchase that item. (Walker, col. 10, lines 10-23).

As the Examiner points out, Walker's system allows a user to establish a price for the product through the computer-based web browser, and reserve the selected product at the local retailer until he purchase the product:

> In addition to the notion of selecting goods and products and establishing prices for the same online, system 100 allows for local store inventory checking and inventory reservations so that a customer knows and is assured that he may acquire a particular product for which he received a price online. Accordingly, after a consumer negotiates a price for a selected product, the consumer is assured that he will actually receive the product when he goes to a selected retailer to acquire that product. As such, system 100 can allow a hold or reservation to be made to reserve an inventory item at a local store. (Walker, col. 10, lines 35-45).

According to Walker, a user can "negotiate" a price for a product through a computer-based web browser by selecting a price set by a manufacturer. The user does not select this price by executing a negotiant function that has been distributed to him, but rather selects the price by performing actions on his own. In Walker, no negotiant function is distributed. In Walker, a consumer does not execute a distributed negotiant function. Therefore the Walker reference does not supply the limitation that is missing from Herz, *i.e.*, distributing the negotiant function to a consumer for execution by the consumer.

For the reasons set forth above, the Applicant respectfully requests this rejection of claim 1 be reversed.

2. Claim 3

Claim 3 is patentable over the combination of Herz and Walker because the combination of Herz and Walker fails to teach receiving a negotiant function and executing the negotiant function.

Claim 3 describes a negotiant function as a function that produces, as an output, an information request designating at least one element of information from among a plurality of elements of information. The specification supports this description of a negotiant function (see for example paragraphs [0038]-[0040] of U.S. Patent Application Publication US 2002/0026345 A1).

For the reasons set forth above for claim 1, neither Herz nor Walker, alone or in combination, teaches a negotiant function. Also for the reasons set forth above for claim 1, neither Herz nor Walker, alone or in combination, teaches receiving a negotiant function or executing the received negotiant function. Accordingly, the Applicant respectfully requests this rejection of claim 3 be reversed.

3. Claim 7

Claim 7 is patentable over the combination of Herz and Walker because the combination of Herz and Walker fails to teach distributing a negotiant function for execution to a plurality of consumers.

As with claim 1, claim 7 describes a negotiant function as a function that accepts elements of data associated with a consumer as input, and produces an information request as output. The specification supports this description of a negotiant function (see for example paragraphs [0038]-[0040] of U.S. Patent Application Publication US 2002/0026345 A1).

For the reasons set forth above for claim 1, neither Herz nor Walker, alone or in combination, teaches a negotiant function. Also for the reasons set forth above for claim 1, neither Herz nor Walker, alone or in combination, teaches distributing a negotiant function for execution to a plurality of consumers. Accordingly, the Applicant respectfully requests this rejection of claim 7 be reversed.

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX. EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

X.   RELATED PROCEEDINGS

No related proceedings are referenced in II. above, or copies of decisions in related proceedings are not provided, hence no Appendix is included.

Respectfully submitted,

Dated: January 11, 2007

Ronald R. Demsher
Registration No.: 42,478
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000 (telephone)
(617) 526-5000 (facsimile)

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/802,278

1.   A method for enabling targeted information retrieval while protecting consumer privacy, the method comprising:

(a)   providing a plurality of elements of information;

(b)   specifying a negotiant function designed to accept a plurality of elements of data associated with a consumer as input and produce an information request as output, said information request designating at least one element of information to present to the consumer from among a plurality of elements of information; and

(c)   distributing the negotiant function to a consumer for execution by said consumer.

2.   The method of claim 1, the method further comprising, after step (c), the steps of

(d)   receiving the information request from said consumer, said information request produced by the negotiant function; and

(e)   transmitting the at least one element of information to the consumer in response to the information request.

3.   A method for enabling targeted information retrieval while protecting consumer privacy, the method comprising:

(a)   receiving a negotiant function for execution, said negotiant function designed to produce an information request as output, the information request designating at least one element of information from among a plurality of elements of information; and

(b)   executing said negotiant function to generate the information request.

4.   The method of claim 3 wherein said negotiant function is designed to accept a plurality of elements of data associated with a consumer as input.

5.   The method of claim 3, the method further comprising, after step (b), the step of transmitting said information request to a source of information.

11

6.   The method of claim 5, the method further comprising, after the transmitting step, the step of receiving at least one element of information from the source of information in response to the information request.

7.   A method for enabling targeted information retrieval while protecting consumer privacy by processing aggregated requests, the method comprising:

      (a)   distributing a negotiant function for execution to a plurality of consumers, the negotiant function designed to produce an information request as output;

      (b)   receiving a plurality of information requests, a first information request of the plurality of information requests associated with a first consumer and obtained by applying a first negotiant function to an element of data associated with the first consumer, a second information request of the plurality of information requests associated with a second consumer and obtained by applying a second negotiant function to an element of data associated with the second consumer.

8.   The method of claim 7, the method further comprising, after step (b), the steps of aggregating a plurality of request pairs, said plurality of request pairs having a sequence, each of said plurality of request pairs comprising an information request and an identifier; and transmitting the plurality of request pairs to a source of information.

9.   The method of claim 7, the method further comprising, after step (b), the steps of encrypting the plurality of information requests; and aggregating a plurality of request pairs V_1, said plurality of request pairs having a sequence, each of said plurality of request pairs comprising an encrypted information request and a consumer identifier.

10.   The method of claim 9, the method further comprising, the step of applying a mix network to said plurality of request pairs V_1 to obtain a plurality of request pairs V_2, the plurality of request pairs V_1 having a first sequence, each of the plurality of request pairs V_1 comprising an information request, said information request encrypted with a first public key and a first random encryption factor, and an identifier, the plurality of request pairs V_2 having a second sequence comprising the first sequence permuted by a first random secret permutation, each of

the plurality of request pairs V_2 comprising the information request in plaintext and the identifier encrypted with a second public key and a second random encryption factor.

11.   The method of claim 10, the method further comprising, the step of replacing the information request in each of the plurality of request pairs V_2 with an element of information to create a plurality of response pairs V_2'.

12.   The method of claim 11, the method further comprising, the step of applying a mix network to the plurality of response pairs V_2' to obtain a plurality of response pairs V_3, the plurality of response pairs V_3 having a third sequence comprising the second sequence permuted by a second random secret permutation, each of the plurality of response pairs V_3 comprising the element of information, said element of information encrypted with a third public key and a third random encryption factor, and the identifier in plaintext.

13.   The method of claim 12, wherein the first public key, the second public key, and the third public key are a single public key.

14.   The method of claim 12, the method further comprising, after step (b), the step of applying asymmetric proxy re-encryption to the plurality of response pairs V_3 to obtain a plurality of response pairs V_4, each of the plurality of response pairs V_4 comprising the element of information encrypted with a fourth public key and the identifier in plaintext.

15.   The method of claim 14 the method further comprising, the step of making the element of information encrypted with the fourth public key available to a consumer based on the identifier.

16.   The method of claim 14 wherein quorum-controlled asymmetric proxy re-encryption is applied to the plurality of response pairs V_3 to obtain a plurality of response pairs V_4, each of the plurality of response pairs V_4 comprising the element of information encrypted with the fourth public key and the identifier in plaintext.

17.   The method of claim 16 wherein the fourth public key is a key of the consumer; and wherein making the element of information encrypted with the fourth key available to the

13

consumer based on the identifier comprises transmitting the element of information encrypted with the fourth public key to the consumer in response to the identifier.

18.   A method for targeted information retrieval while protecting consumer privacy by comparing blinded ciphertexts, the method comprising:

         (a)   distributing a negotiant function for execution to a plurality of consumers, the negotiant function designed to produce an information request as output;

         (b)   receiving a request pair in response to the negotiant function, the request pair comprising a consumer identifier and the information request and a first random encryption factor, the information request encrypted with the first public key and the first random encryption factor having a first underlying plaintext;

         (c)   constructing a first plurality of information pairs, the first plurality of information pairs having a first sequence, each of the first plurality of information pairs comprising an element identifier and an element of information encrypted with a second public key and a second random encryption factor;

         (d)   applying a mix network to the first plurality of information pairs to obtain a second plurality of information pairs, the second plurality of information pairs having a second sequence comprising the first sequence permuted by a random secret permutation, each of the second plurality of request pairs comprising the element identifier encrypted with a third public key and a third random encryption factor and the element of information re-encrypted with the third public key and the third random encryption factor, the element identifier encrypted with the third public key and the third random encryption factor having a second underlying plaintext; and

         (e)   performing a distributed plaintext equality test to identify at least one of the second plurality of request pairs in which the second underlying plaintext is identical to the first underlying plaintext.

19.   The method of claim 18 wherein the first public key, the second public key, and the third public key are a single public key.

20.   The method of claim 18, the method further comprising, after step (e), the step of applying asymmetric proxy re-encryption to the at least one of the second plurality of request

pairs in which the second underlying plaintext is identical to the first underlying plaintext to obtain at least one response pair, each of the at least one response pair comprising the element of information encrypted with a fourth public key and the consumer identifier.

21.   The method of claim 20 wherein quorum-controlled asymmetric proxy re-encryption is applied to the at least one of the second plurality of request pairs in which the second underlying plaintext is identical to the first underlying plaintext to obtain at least one response pair, each of the at least one response pair comprising the element of information encrypted with the fourth public key and the consumer identifier.

22.   The method of claim 21, the method further comprising, after step (e), the step of making the element of information encrypted with the fourth public key available to the consumer based on the consumer identifier.

23.   The method of claim 22 wherein the step of making the element of information encrypted with the fourth public key available to the consumer based on the consumer identifier comprises transmitting the element of information encrypted with the fourth public key to the consumer in response to the consumer identifier.

15